From Incident Response to Operational Resilience

Mohanraj Gunasekaran | Major Incident Management • IT Service Operations • Problem Management

Executive Summary

Resilient IT operations require more than rapid technical restoration. A repeatable model combines business-impact assessment, incident command, coordinated technical work, controlled recovery, clear stakeholder communication and evidence-led learning.

1. Operating Principles

Impact-led prioritisation; a single coordination point; clear technical ownership; fact/hypothesis separation; time-boxed actions; controlled recovery; and consistent updates.

2. Incident Lifecycle

Detect and record → assess impact and classify → mobilise roles and workstreams → contain and restore safely → validate and communicate → close and review.

3. Command and Accountability

Incident Manager coordinates response, priorities, decisions, escalations and communications. Technical leads guide investigation and remediation. Service/business representatives validate impact and recovery. Problem Management drives systemic analysis and action follow-through. Change governance applies to production changes.

4. Communication

Updates should state confirmed impact, scope, current status, actions and owners, risks/unknowns, decisions required and the next update time. Avoid speculative root cause statements and distinguish service restoration from full resolution.

5. RCA and Problem Management

Build a time-stamped evidence-based timeline; test causal hypotheses; identify contributing conditions and control gaps; assign corrective/preventive actions with owners, dates and success criteria; and review effectiveness after implementation.

6. Governance Metrics

Potential measures include time to acknowledge, time to restore, update timeliness, service availability, repeat incident rate, RCA completion, action aging and change-related incident rate. Define scope, data source, clock rules, exclusions and target before comparing.

7. 30–60–90 Day Roadmap

Days 1–30: establish baselines, review critical services and standardise response. Days 31–60: pilot improvements to RCA, action tracking, communications and change linkage. Days 61–90: embed governance, evaluate effectiveness and prioritise the next improvement cycle.

Conclusion

Operational resilience is a continuous management discipline. Consistent command, transparent communication, evidence-led learning and measurable follow-up turn incident response into sustained service improvement.

Professional practice sample. Generic, public-safe content; not employer documentation.